Symantec AntiVirus™ Corporate Edition Reference Guide

Symantec AntiVirus™ Corporate Edition Reference Guide

Documentation version 9.0

Copyright Notice

Trademarks

Printed in the United States of America.
10 9 8 7 6 5 4 3 2 1

Technical support

As part of Symantec Security Response, the Symantec global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/ function, installation, and configuration, as well as to author content for our Web-accessible Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering as well as Symantec Security Response to provide Alerting Services and virus definitions updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages for those customers enrolled in the Platinum Support Program
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, offer enhanced response and proactive security support

Please visit our Web site for current information on Support Programs. The specific features available may vary based on the level of support purchased and the specific product that you are using.

Licensing and registration

If the product that you are implementing requires registration and/or a license key, the fastest and easiest way to register your service is to access the Symantec licensing and registration site at www.symantec.com/certificate. Alternatively, you may go to www.symantec.com/techsupp/ent/enterprise.html, select the product that you wish to register, and from the Product Home Page, select the Licensing and Registration link.

Contacting Technical Support

Customers with a current support agreement may contact the Technical Support group via phone or online at www.symantec.com/techsupp.

Customers with Platinum support agreements may contact Platinum Technical Support via the Platinum Web site at www-secure.symantec.com/platinum/.

When contacting the Technical Support group, please have the following:

- Product release level
- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
  - Error messages/log files
  - Troubleshooting performed prior to contacting Symantec
  - Recent software configuration changes and/or network changes

Customer Service

To contact Enterprise Customer Service online, go to www.symantec.com, select the appropriate Global Site for your country, then choose Service and Support. Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

Contents

Chapter 1

Introducing the reference guide

This chapter includes the following topics:

This reference guide contains technical product information for Symantec AntiVirus, including information on tools that are on the Symantec AntiVirus CD. It is intended for system administrators and others who install and maintain this product in a networked, corporate environment.

What is in the reference guide

Table 1-1 lists and describes the topics in this reference guide.

Table 1-1 Reference guide topics

Topic	Description
Scenarios	This chapter provides examples of how Symantec AntiVirus is implemented in four different-sized organizations: small, medium, large, and enterprise. Although your particular situation may not precisely match any of the examples, you can get an idea of how others have implemented security solutions, and what types of issues influenced their choices.
Reset ACL tool	Many of the configuration settings for Symantec AntiVirus are stored in the Windows registry. Reset ACL lets you restrict access to these registry settings on Windows XP/2000/NT operating systems to prevent unauthorized users from making changes.

Table 1-1 Reference guide topics

Topic	Description
Importer tool	The Importer tool is a command-line utility specifically for use with the Symantec System Center. The Importer tool lets you import as many sets of computer names and IP addresses into a special address cache as you need. Symantec AntiVirus can then locate computers during the Discovery process in situations where the computer names cannot be resolved using WINS/DNS.
Windows XP/2000/ NT services	This chapter lists the names of services run automatically by Symantec AntiVirus and the Symantec System Center. Those names appear in the Windows XP/2000/NT Services control panel.
Windows XP/2000/ NT Event Log entries	This chapter lists the events written by Symantec AntiVirus to the Windows XP/2000/NT Event Log.

Chapter 2

User scenarios

This chapter includes the following topics:

About user scenarios

The user scenarios describe methods for implementing Symantec AntiVirus in different sized organizations. The scenarios present commonly used methods but do not cover all possible strategies.

Scenario 1: Small-sized organization

This organization has one office. The organization's environment includes the following:

- The organization has less than 250 nodes, the majority of which run Windows 2000/XP.
- The organization uses a Microsoft Exchange server for email and is running Microsoft Outlook as its client mail program.
- The organization has a major industry-specific application that Management Information Systems (MIS) runs on another server in the organization.
- Microsoft Office is used throughout the organization.

How small organizations roll out Symantec AntiVirus

Small organizations roll out Symantec AntiVirus in the following ways:

- Symantec AntiVirus is rolled out from the Symantec System Center console. When installing from the Symantec System Center console, MIS uses Elevated Privileges rather than granting administrative privileges to the user on the target computer.
- Remote users are given a CD to install an unmanaged Symantec AntiVirus client.

How small organizations manage alerting

Depending on the organization's size, alerting can be managed from the Symantec System Center console using the Alert Management System^2 (AMS^2). This requires an MIS administrator who has the bandwidth to centrally manage Symantec AntiVirus.

For clients that are managed from the Symantec System Center console:

- The primary server runs AMS^2. The administrator receives a notification when a virus is found. Notifications can be sent in the form of a message box, network broadcast, or page. AMS^2 can also run a program, write to the Windows Event Log, send an SNMP trap, or load an NLM.
- AMS^2 logs are monitored from the Symantec System Center for events or viruses that might require extra attention.

MIS installs the AMS^2 client program on unmanaged clients to use the alerting features that AMS^2 provides. The unmanaged clients then forward their alerts to an AMS^2 server.

For clients that are not managed centrally:

- A notification is sent to an administrator's account when a virus is found. Notifications can be sent in the form of a message box, network broadcast, or page. AMS^2 can also run a program, write to the Windows Event Log, send an SNMP trap, or load an NLM.
- AMS^2 logs are monitored from the Alert Management System^2 console for events or viruses that might require extra attention.

How small organizations protect their environments from threats

Small organizations protect their environments from threats in several ways.

For computers that are managed from the Symantec System Center console:

- The Symantec AntiVirus server program is installed on a single nonproduction Windows 2000 server, which is the primary server. All other network servers are protected by Symantec AntiVirus client.
- All workstations are protected by Symantec AntiVirus client.
- MIS defines the Symantec AntiVirus options for workstations. MIS locks the options to prevent users from changing how Symantec AntiVirus protects their computers from viruses.
- MIS installs the Symantec System Center on a Windows 2000 Professional computer for antivirus administration.
- The primary server receives updates automatically using LiveUpdate. It uses the Virus Definition Transport Method to push virus definitions to all managed clients.
- MIS groups workstations that it considers to be less secure in the same client group. The Symantec AntiVirus settings for this client group provide the workstations with a higher level of protection than other workstations.
- MIS enables expanded threat detection so that programs such as spyware and adware are detected.
- Threat alerts and virus definitions updates are monitored regularly from the Symantec System Center console.
- MIS regularly checks the Event Log and Threat History for any events, viruses, or other threats, such as adware or spyware, that might require special attention.
- Auto-Protect SmartScan and scanning are enabled and locked down on all computers.
- In-memory scanning is enabled to address virus-infected files that are associated with a running process.
- File caching is enabled on all computers to improve scanning times.
- Internet email is enabled on all computers with Internet email accounts.
- Threat Tracer is enabled on computers with network shares so that system administrators can identify the source of network share-based virus infections on computers that are running Windows NT/2000/XP operating systems.

- Users access files on file and application servers often. By default, Auto-Protect scans files when they are created, renamed, moved, opened, copied, executed, or saved. MIS configures Auto-Protect to scan files only when they are created, renamed, or moved. This improves performance because the number of file operations that are monitored is reduced.
- The administrator schedules a scan of all network servers during nonproduction hours. The scan is scheduled to run at a different time than the scheduled nightly backup so that they do not interfere with each other.
- The administrator schedules a weekly scan of all workstations and configures Symantec AntiVirus so that users cannot cancel the administrator-scheduled scan.

For computers that are not managed centrally:

- All computers are protected by Symantec AntiVirus. The computers use the Symantec AntiVirus options that are defined by MIS. MIS uses the Configuration Editor (Configed.exe) to configure Symantec AntiVirus options and locks them to prevent users from changing how Symantec AntiVirus protects their computers from viruses. The Configuration Editor is an unsupported tool that is located on the CD in the Tools\Nosuprt folder.
- MIS enables expanded threat detection on all computers so that programs such as spyware and adware are detected.
- Auto-Protect SmartScan is enabled and locked down on all computers.
- In-memory scanning is enabled to address virus-infected files that are associated with a running process.
- File caching is enabled on all computers to improve scanning times.
- Internet email scanning is enabled on all computers with Internet email accounts.

How small organizations update their virus definitions

Small organizations update their virus definitions in several ways.

For computers that are managed from the Symantec System Center console:

- Some Symantec AntiVirus clients automatically receive virus definitions from their parent server using the Virus Definition Transport Method. When the parent server receives new virus definitions, it immediately begins sending the clients definitions updates. The parent server is able to update multiple clients at a time, and simultaneously updates one client on each subnet to reduce network traffic.
- The Windows 2000 primary servers automatically retrieve virus definitions updates directly from Symantec. This occurs on a scheduled or on-demand basis.
- When an update operation that was performed at the server group level succeeds on all but a few clients, MIS forces the failed clients to update virus definitions files immediately using LiveUpdate.

Computers that are not managed centrally retrieve virus definitions directly from Symantec by running LiveUpdate.

How small organizations ensure that clients are compliant with the corporate security policy

Small organizations ensure that clients are compliant with the corporate security policy in several ways.

For computers that are managed centrally, MIS uses the Symantec System Center to change and lock down policy settings.

For computers that are not managed centrally:

- MIS uses the Configuration Editor (Configed.exe) to configure Symantec AntiVirus options and locks them to prevent users from changing how Symantec AntiVirus protects their computers from viruses. The Configuration Editor is an unsupported tool that is located on the CD in the Tools\Nosuprt folder.
- Auto-Protect is locked down.
- Administrator-scheduled scans are set and locked down.
- Scheduled LiveUpdate is set and locked down.

- On computers that connect to the network using a VPN connection, MIS installs Symantec VPN Sentry. Symantec VPN Sentry performs a client compliancy check to verify that:
  - Auto-Protect is enabled.
  - Auto-Protect heuristic virus scanning is enabled and is at the specified level or higher.
  - Auto-Protect is configured to scan specified types of file access.
  - A LiveUpdate session is completed successfully within a specified number of days.
  - The installed Symantec AntiVirus version is the specified version or later.
  - Virus definitions files are no older than a specified maximum age.
  - A specified scan ran within the last (n) days.
  - The Microsoft Exchange/Outlook plug-in scanner is installed and enabled.
  - The Lotus Notes plug-in scanner is installed and enabled.

When virus definitions files are older than required or when Auto-Protect and heuristic virus scanning are disabled, client compliancy remediates the VPN client automatically. When the version of Symantec AntiVirus is too old, the issue is logged. In low risk environments, the client is allowed network access and the user is notified to upgrade. In high risk environments, the client is denied access and the user is notified to upgrade.

Scenario 2: Medium-sized organization

This organization has one office and several remote users. The organization's environment includes the following:

- The organization has a total of 1,000 workstations, 96% of which run Windows 2000/XP. The remainder of the workstations run Windows 98/Me.
- Several users work remotely from their home computers, which run Windows 2000/XP.
- Currently, 98% of the organization's servers are Windows 2003. There are several NetWare servers in the organization.
- Microsoft Word and Microsoft Excel are used throughout the organization.

How medium-sized organizations roll out Symantec AntiVirus

Medium-sized organizations roll out Symantec AntiVirus in the following ways:

- Symantec AntiVirus server and client are rolled out from the Symantec System Center console. When installing from the Symantec System Center console, MIS uses Elevated Privileges rather than granting administrative privileges.
- Logon scripts are set up to run silent installations of Symantec AntiVirus client if the product is not detected on the computer.
- Some client installation is Web-based.
- Remote users are given a CD to install an unmanaged Symantec AntiVirus client.

How medium-sized organizations manage alerting

Medium-sized organizations manage alerting in the following ways:

- AMS^2 is installed on the primary server. An email is sent to an administrator's account when a virus is found.
- AMS^2 logs are monitored from the Symantec System Center for events or viruses that might require extra attention.

How medium-sized organizations protect their environments from threats

Medium-sized organizations protect their environments from threats in the following ways:

- The Symantec AntiVirus server program is installed on a single nonproduction Windows 2003 server, which is the primary server. All other Windows-based network servers are protected by Symantec AntiVirus client. All NetWare servers run Symantec AntiVirus server.
- All workstations are protected by Symantec AntiVirus client. The workstations use the Symantec AntiVirus options defined by MIS. MIS locks Symantec AntiVirus options to prevent users from changing how Symantec AntiVirus protects their computers from viruses. Auto-Protect is configured to load on system startup, and then unload on system shutdown. SmartScan, clean file caching, and Threat Tracer are enabled.
- POP3 and SMTP Internet email scanning are enabled on all computers with Internet email accounts.

- MIS installs the Symantec System Center on a Windows 2000 Professional computer for antivirus administration.
- Workstations that MIS considers to be less secure are members of the same client group. MIS configures the Symantec AntiVirus settings for this client group to provide the workstations with a higher level of protection than other workstations.
- MIS enables expanded threat detection on all computers so that programs such as spyware and adware are detected.
- Threat alerts and virus definitions updates are monitored regularly from the Symantec System Center console. MIS regularly checks the Event Log and Threat History for any events, viruses, or other threats, such as adware or spyware, that might require extra attention.
- Most of the servers are file and application servers. Users access files on these servers often. By default, Auto-Protect scans files when they are created, renamed, moved, opened, copied, executed, or saved. MIS configures Auto-Protect to scan files only when they are created, renamed, or moved. This improves performance because the number of file operations that are monitored is reduced.
- The administrator schedules a scan of all network servers during nonproduction hours. The scan is scheduled to run at a different time than the scheduled nightly backup so that they do not interfere with each other.
- The administrator schedules a weekly scan of all workstations and configures Symantec AntiVirus so that users cannot cancel the administrator-scheduled scan.

How medium-sized organizations update their virus definitions

Medium-sized organizations update their virus definitions in the following ways:

- A central LiveUpdate server is placed in the environment from which all clients and servers retrieve virus definitions updates. The updates are randomly scheduled to reduce network bandwidth. The LiveUpdate server automatically retrieves virus definitions directly from Symantec. Clients pull virus definitions updates from the internal LiveUpdate server.
- Remote clients retrieve definitions updates from Symantec by running LiveUpdate.
- When an update operation that was performed at the server group level succeeds on all but a few clients, MIS forces the failed clients to update virus definitions files immediately using LiveUpdate. This method works to

remediate clients that normally receive updates using LiveUpdate or the Virus Definition Transport Method.

How medium-sized organizations ensure that clients are compliant with the corporate security policy

Medium-sized organizations ensure that clients remain compliant with the corporate security policy in several ways.

For computers that are managed centrally, MIS uses the Symantec System Center to change and lock down policy settings.

For computers that are not managed centrally:

- MIS uses the Configuration Editor (Configed.exe) to configure Symantec AntiVirus options and locks them to prevent users from changing how Symantec AntiVirus protects their computers from viruses. The Configuration Editor is an unsupported tool that is located on the CD in the Tools\Nosuprt folder.
- Auto-Protect is locked down.
- Administrator-scheduled scans are set and locked down.
- Scheduled LiveUpdate is set and locked down.
- On computers that connect to the network using a VPN connection, MIS installs Symantec VPN Sentry. Symantec VPN Sentry performs a client compliancy check to verify that:
  - Auto-Protect is enabled.
  - Auto-Protect heuristic virus scanning is enabled and is at the specified level or higher.
  - Auto-Protect is configured to scan specified types of file access.
  - A LiveUpdate session is completed successfully within a specified number of days.
  - The installed Symantec AntiVirus version is the specified version or later.
  - Virus definitions files are no older than a specified maximum age.
  - A specified scan ran within the last (n) days.
  - The Microsoft Exchange/Outlook plug-in scanner is installed and enabled.
  - The Lotus Notes plug-in scanner is installed and enabled.

When virus definitions files are older than required or when Auto-Protect and heuristic virus scanning are disabled, client compliancy remediates the VPN client automatically. When the version of Symantec AntiVirus is too old, the

issue is logged. In low risk environments, the client is allowed network access and the user is notified to upgrade. In high risk environments, the client is denied access and the user is notified to upgrade.

Scenario 3: Large-sized organization

This organization has one corporate office and 50 branch offices scattered across the New England states. The organization's environment includes the following:

- The corporate office has 5,000 workstations that are located in five buildings. Each of the branch offices averages about 100 workstations.
- There are 420 servers in the organization, 98% of which are Windows 2000 and 2% of which are NetWare. Most of the servers are located at the corporate office, so many branch offices do not have local servers. There are two Terminal Servers.
- The organization has a total of 10,000 workstations, 70% of which are Windows 2000 and 30% of which are Windows 98/Me/XP.
- There are 60 thin clients connected to the Terminal Servers.
- The branch offices are connected to the corporate office through a 56-KB wide area network (WAN) link, and the corporate office has a 128-KB link to the Internet. Because of limited bandwidth, it is important to keep network traffic on these links to a minimum.
- Microsoft Exchange, Microsoft Word, and Microsoft Excel are used throughout the organization. Most of the organization's workstations are highly susceptible to macro viruses, viruses spread through email, and blended threats.

How large organizations roll out Symantec AntiVirus

Large organizations roll out Symantec AntiVirus installations in the following ways:

- At their corporate headquarters, MIS rolls out Windows Installer (.msi) installation and migration packages for Symantec AntiVirus client to local computers using a third-party tool. When setting up the packages, MIS chose to install silently.
- Users at the branch offices use a Web-based installation method for installing Symantec AntiVirus client. MIS sent these users email messages with instructions and a URL link to the Web-based installer.
- Symantec AntiVirus server is rolled out from the Symantec System Center console.

How large organizations manage alerting

Large organizations manage alerting in the following ways:

- Each primary server is also an AMS^2 server. All other server (including Terminal Server Console) and workstation alerts are forwarded to these servers.
- When a virus is found, AMS^2 emails the administrator in charge of antivirus protection.
- AMS^2 logs are monitored from the Symantec System Center for events, viruses, or blended threats that might require extra attention.

How large organizations protect their environments from threats

Large organizations protect their environments from viruses in the following ways:

- To guard its site from infections originating on the Internet, MIS runs Symantec Enterprise Firewall. Symantec AntiVirus POP3 and SMTP Internet email scanning are also enabled on all computers with Internet email accounts.
- The Microsoft Exchange server is protected by Symantec Mail Security for Microsoft Exchange.
- The Symantec System Center console is installed at the corporate office so the administrators can configure antivirus settings from a central location.
- All NetWare servers are protected by Symantec AntiVirus server.

- All Windows NT/2000 servers that manage Symantec AntiVirus clients are protected by Symantec AntiVirus server. All other Windows NT/2000 servers are protected by Symantec AntiVirus client.
- Symantec AntiVirus server runs on the Terminal Servers.
- All workstations are protected by Symantec AntiVirus client. The workstations use the Symantec AntiVirus options defined by the MIS group. Email is scanned by the Symantec AntiVirus email plug-in. MIS locks Symantec AntiVirus options to prevent users from changing the way that their computers are protected from viruses. Auto-Protect is configured to load on system startup, and then unload on system shutdown. SmartScan, file caching, and Threat Tracer are enabled.
- MIS enables expanded threat detection on computers so that programs such as spyware and adware are detected.
- Threat alerts and virus definitions updates are monitored regularly from the Symantec System Center console. MIS regularly checks the Event Log and Threat History for any events, viruses, or other threats, such as adware or spyware, that might require extra attention.
- MIS sets up multiple Symantec AntiVirus server groups and client groups. Before setting up server groups and client groups, MIS created a comprehensive plan. The plan addressed numerous issues, such as physical server requirements, link speeds, and the security levels that are required for departments and groups with varying needs and levels of vulnerability.
- Servers that are running Symantec AntiVirus server are divided into several different server groups. For example, all Terminal Servers and NetWare servers that are running Symantec AntiVirus server are members of the same server group because they share common functions, load, and overhead requirements.
- Client groups have been set up for different departments. For example, computers in the Development group are assigned to a client group with lower-level security settings. Computers in the Customer Service department are highly susceptible to email viruses. These computers are organized into a client group with high-level Symantec AntiVirus product settings. All Symantec AntiVirus client settings are locked.
- Some local and remote clients are separated into different client groups because they use different virus definitions updating methods.

- Windows NT/2000 servers that do not act as parent servers run Symantec AntiVirus client. Users access files on these servers often. By default, Auto-Protect scans files when they are created, renamed, moved, opened, copied, executed, or saved. MIS configures Auto-Protect to scan files only when they are created, renamed, or moved. This improves performance because the number of file operations that are monitored is reduced.
- Clients are configured so that when File System Auto-Protect is disabled by a user, it is automatically reenabled after 30 minutes.
- Symantec AntiVirus is configured to forward infected files that cannot be repaired to a Central Quarantine Server. The administrator submits suspicious files to Symantec Security Response for analysis. Symantec Security Response analyzes the file submissions and reports back to the administrator with new virus definitions or other solutions.
- The administrator schedules a scan for all computers that are running Symantec AntiVirus server during nonproduction hours. The antivirus scan is scheduled to run at a different time than the scheduled nightly backup so that they do not interfere with each other.
- Administrators schedule scans to run every five days. In the Client Administrator Only Options dialog box, Symantec AntiVirus is configured to snooze scheduled scans when the client is running on a battery; this way, if a laptop is running on batteries, a scheduled scan will wait until the laptop is back on AC power.
- For scheduled and manual scans, CPU utilization is configured on Windows computers based on when they are idle and not idle. The idle setting allows for higher CPU utilization when the computer is idle. The not idle setting is set for lower CPU utilization, which minimizes the impact on user productivity.

How large organizations update their virus definitions

Large organizations update their virus definitions in the following ways:

- MIS implements an approach that reduces traffic to the Internet. The administrator selects an established FTP server that makes up part of the company intranet to act as a LiveUpdate server. This is not a dedicated LiveUpdate or Symantec AntiVirus server. The LiveUpdate Administration Utility pulls Symantec AntiVirus product updates and virus definitions files from the Symantec FTP site to the FTP server in the corporate office.
- The LiveUpdate Administration Utility is scheduled to download new packages daily, after hours.

- The primary servers retrieve virus definitions updates from the internal LiveUpdate server. They then push the virus definitions updates to the secondary servers.
- Parent servers push the clients' virus definitions updates using the Virus Definition Transport Method. The virus definitions file size is small. MIS configures Symantec AntiVirus to deliver the virus definitions files efficiently. The push is multi-threaded, from fastest to slowest. Each thread deploys to one subnet at a time until all clients on that subnet have been served.
- When an update operation that was performed at the server group level succeeded on all but a few clients, MIS forces the failed clients to update virus definitions files immediately using LiveUpdate. This method works to remediate clients that normally receive updates using LiveUpdate or the Virus Definition Transport Method.

How large organizations ensure that clients are compliant with the corporate security policy

Large organizations ensure that clients are compliant with the corporate security policy in several ways.

For computers that are managed centrally, MIS uses the Symantec System Center to change and lock down policy settings.

For computers that are not managed centrally:

- MIS uses the Configuration Editor (Configed.exe) to configure Symantec AntiVirus options and locks them to prevent users from changing how Symantec AntiVirus protects their computers from viruses. The Configuration Editor is an unsupported tool that is located on the CD in the Tools\Nosuprt folder.
- Auto-Protect is locked down.
- Administrator-scheduled scans are set and locked down.
- Scheduled LiveUpdate is set and locked down.
- On computers that connect to the network using a VPN connection, MIS installs Symantec VPN Sentry. Symantec VPN Sentry performs a client compliancy check to verify that:
  - Auto-Protect is enabled.
  - Auto-Protect heuristic virus scanning is enabled and is at the specified level or higher.
  - Auto-Protect is configured to scan specified types of file access.

- A LiveUpdate session is completed successfully within a specified number of days.
- The installed Symantec AntiVirus version is the specified version or later.
- Virus definitions files are no older than a specified maximum age.
- A specified scan ran within the last (n) days.
- The Microsoft Exchange/Outlook plug-in scanner is installed and enabled.
- The Lotus Notes plug-in scanner is installed and enabled.

When virus definitions files are older than required or when Auto-Protect and heuristic virus scanning are disabled, client compliancy remediates the VPN client automatically. When the version of Symantec AntiVirus is too old, the issue is logged. In low risk environments, the client is allowed network access and the user is notified to upgrade. In high risk environments, the client is denied access and the user is notified to upgrade.

Scenario 4: Enterprise-sized organization

This organization has offices around the world. The organization has 150 offices in the United States, ranging from 20 to 3,000 employees. The organization's environment includes the following:

- The organization has 2,500 servers, of which 10% run NetWare, 20% Windows NT, 65% Windows 2000, and 5% UNIX.
- The organization has a total of 35,000 workstations in the United States, of which 50% run Windows 98/Me/XP and 50% run Windows NT/2000.
- Many Windows NT/2000 users do not have administrative rights to their workstations.
- Many of the Windows computers are laptops.
- A small number of workstations are 64-bit computers that use Windows XP 64-Bit Edition 2003.
- Lotus Notes, Microsoft Exchange, Microsoft Word, and Microsoft Excel are used throughout the organization.

This organization uses Tivoli SecureWay Risk Manager 3.7, which ships with an adapter for Symantec AntiVirus. This adapter allows Tivoli SecureWay Risk Manager to read the Symantec AntiVirus Event Log. Information gathered and displayed by Tivoli SecureWay Risk Manager includes the status of virus definitions updates, historical information on scans, and statistics regarding the number of infections within the organization.

How enterprise-sized organizations roll out Symantec AntiVirus

Enterprise-sized organizations roll out Symantec AntiVirus in the following ways:

- MIS rolls out Windows Installer (.msi) installation and migration packages with customized command-line options for most local computers using Active Directory. Different packages from different parent servers are distributed to each client group, depending on the location and special needs of those clients.
- In some cases, MIS installs Symantec AntiVirus from the Symantec System Center console. MIS uses Elevated Privileges rather than granting administrative privileges to the user on the target computer.
- MIS creates a special Symantec AntiVirus installation CD for laptop users that contains a similar installation package.
- Small branch offices that do not utilize SMS use a Web-based installation method to distribute the installation packages. MIS sent these users email messages with instructions and a URL link to the Web-based installer.

How enterprise-sized organizations manage alerting, logging, and reporting

Enterprise-sized organizations manage alerting, logging, and reporting in the following ways:

- Symantec AntiVirus clients are configured to limit the types of events that they forward to parent servers. Symantec AntiVirus is configured on secondary servers to forward only the events that MIS cares about to primary servers.
- Symantec AntiVirus events are forwarded from primary servers to the Symantec management console via the Symantec AntiVirus Collector. MIS uses the Symantec management console to log events, create alert notifications as responses to events, and generate predefined and custom reports that contain event status.
- Thresholds have been set to manage the alerts and notifications. MIS uses pagers, email, and SNMP traps for alert notifications.
- MIS queries, filters, and sorts events to determine which systems are not protected, out-of-date, or have high-severity events occurring on them.
- MIS generates tabular and graphical reports of event status, based on filtered views that the MIS department has created. Some reports are for its own use, while others for MIS directors and corporate upper management.

How enterprise-sized organizations protect their environments from threats

Enterprise-sized organizations protect their environments from threats in the following ways:

- To guard its site from infections originating in Internet email, MIS runs Symantec AntiVirus for SMTP Gateways. Symantec AntiVirus POP3 and SMTP Internet email scanning are also enabled on all computers with Internet email accounts.
- Lotus Notes servers are protected by Symantec Mail Security for Domino.
- Microsoft Exchange servers are protected by Symantec Mail Security for Microsoft Exchange.
- All NetWare servers are protected by the Symantec AntiVirus server program.
- All 64-bit computers are protected by Symantec AntiVirus client.
- Most Windows NT/2000 servers are protected by Symantec AntiVirus client. The few dedicated servers that are part of the enterprise antivirus deployment are protected by Symantec AntiVirus server. NetWare servers and Terminal Servers are also protected by Symantec AntiVirus server.
- All workstations are protected by Symantec AntiVirus client. The workstations use the Symantec AntiVirus options defined by MIS. Expanded threat detection is enabled for all categories. POP3 and SMTP email client protection, outbound email heuristics scanning, and in-memory threat scanning are enabled. Auto-Protect is configured to load on system startup, and then unload on system shutdown. SmartScan, file caching, and Threat Tracer are enabled.
- MIS locks Symantec AntiVirus options to prevent users from changing the way that Symantec AntiVirus protects their computers from viruses. Special antivirus configurations are assigned to client groups with special needs, such as those where security risks are high.
- Branch offices with fast links are under one server group with multiple client groups for different departments.
- Some branch offices with slow links have their own server groups. The administrator at each of these sites is responsible for the antivirus protection at that site. Some branch offices with slow links have their own parent servers rather than server groups. They use the Virus Definition Transport Method. The primary server, which is located at the corporate data center, delivers the virus definitions files over a 56-KB link. The parent servers push the virus definitions files to clients over the branch's local area

network (LAN). In small branches that do not have a server, clients are assigned to a remote parent server. The clients are configured to run LiveUpdate on a randomized basis. The clients are configured to check if a LiveUpdate session was scheduled to run when the client was unavailable; if so, the client runs LiveUpdate once the computer starts up.

- Nearly all of Symantec AntiVirus is managed at the corporate MIS office. MIS maintains standard and consistent client security policies.
- There are administrators at the largest branch offices with slow links. The Symantec System Center console runs at corporate MIS and at these offices only. The branch administrators have the passwords for the server groups for which they are responsible.
- Client groups are set up to provide the appropriate level of protection. The Sales department is located in four different offices. All of their client computers are members of the Sales client group. The Development department is located in one office but also has its own client group. Their antivirus options are less restrictive so they can disable antivirus protection when compiling a program.
- Windows NT/2000 servers that do not act as parent servers run Symantec AntiVirus client. Users access files on these servers often. By default, Auto-Protect scans files when they are created, renamed, moved, opened, copied, executed, or saved. MIS configures Auto-Protect to scan files only when they are created, renamed, or moved. This improves performance because the number of file operations that are monitored is reduced.
- Laptop users are set up as roaming clients. When they do connect to the internal network through a modem, they are assigned the best parent server based on proximity and speed. Symantec AntiVirus checks for updates and may receive a small settings file to update options.
- Workstations that do not fall into a special-needs category share a parent server. There are no more than 5,000 clients attached to each parent server. These clients check in with their parent server every 200 minutes.
- Symantec AntiVirus forwards unrepairable infected files to a Central Quarantine Server. Suspicious files are forwarded to Symantec Security Response through the Digital Immune System (DIS) for analysis. DIS analyzes the file submissions, and then either returns new virus definitions available at the DIS gateway or submits the file to Symantec Security Response for further analysis.
- Clients are configured so that when File System Auto-Protect is disabled by a user, it is automatically reenabled after 30 minutes.

- The administrator schedules a Server Group Scan to scan all computers that are running the Symantec AntiVirus server program during nonproduction hours. The antivirus scan is scheduled to run at a different time than the scheduled nightly backup so they do not interfere with each other.
- The administrator schedules a weekly Client Scan. In the Client Administrator Only Options dialog box, Symantec AntiVirus is configured to snooze scheduled scans when the client is running on a battery; this way, if a laptop is running on batteries, a scheduled scan will wait until the laptop is back on AC power.
- For the Sales client group, the administrator configures the scheduled scan to allow the salesperson to delay the scan. If the scheduled scan starts during a task like a presentation, the salesperson can click the Snooze button to delay the scan for three hours. The salesperson may use the snooze button two times before the scheduled scan runs.
- For scheduled and manual scans, CPU utilization is configured on Windows computers based on when they are idle and not idle. The idle setting allows for higher CPU utilization when the computer is idle. The not idle setting is set for lower CPU utilization, which minimizes the impact on user productivity.

How enterprise-sized organizations update their virus definitions

Enterprise-sized organizations update their virus definitions in the following ways:

- One Windows 2000 server in the central office is designated as a master primary server. This server receives definitions updates from Symantec using a scheduled LiveUpdate.
- The primary servers pull from the master primary server at their scheduled time and frequency. The primary servers push the virus definitions files to the parent servers. The parent server updates multiple clients at a time, and simultaneously updates one client on each subnet to reduce network traffic.
- 64-bit computers are configured to use Continuous LiveUpdate, which automatically forces a computer to look for new updates when the virus definitions files have exceeded a specified age.

- Most mobile users receive virus definitions from their assigned roaming parent server. The virus definitions files are small and do not take a long time to transfer across a dial-up connection. Mobile users also use Continuous LiveUpdate as a backup option for receiving updates directly from Symantec whenever the computer connects to the Internet. MIS has specified a maximum number of days that the virus definitions files on a Symantec AntiVirus computer can be out-of-date before forcing an update. When Symantec AntiVirus client determines that its virus definitions files have exceeded their maximum age, it initiates a silent LiveUpdate session when it detects that an Internet connection is available.
- Dial-up mobile users have a logon script or a RAS/VPN script that triggers LiveUpdate to update virus definitions files once the user is authenticated to the RAS/VPN server.
- When an update operation that was performed at the server group level succeeds on all but a few clients, MIS forces the failed clients to update virus definitions files immediately using LiveUpdate. This method works to remediate clients that normally receive updates using LiveUpdate or the Virus Definition Transport Method.

How enterprise-sized organizations ensure that clients are compliant with the corporate security policy

Enterprise-sized organizations ensure that clients are compliant with the corporate security policy in several ways.

For computers that are managed centrally, MIS uses the Symantec System Center to change and lock down policy settings at the server group level.

For computers that are not managed centrally:

- MIS uses the Configuration Editor (Configed.exe) to configure Symantec AntiVirus options and locks them to prevent users from changing how Symantec AntiVirus protects their computers from viruses. The Configuration Editor is an unsupported tool that is located on the CD in the Tools\Nosuprt folder.
- Auto-Protect is locked down.
- Administrator-scheduled scans are set and locked down.

- Scheduled LiveUpdate is set and locked down.
- On computers that connect to the network using a VPN connection, MIS installs Symantec VPN Sentry. Symantec VPN Sentry performs a client compliancy check to verify that:
  - Auto-Protect is enabled.
  - Auto-Protect heuristic virus scanning is enabled and is at the specified level or higher.
  - Auto-Protect is configured to scan specified types of file access.
  - A LiveUpdate session is completed successfully within a specified number of days.
  - The installed Symantec AntiVirus version is the specified version or later.
  - Virus definitions files are no older than a specified maximum age.
  - A specified scan ran within the last (n) days.
  - The Microsoft Exchange/Outlook plug-in scanner is installed and enabled.
  - The Lotus Notes plug-in scanner is installed and enabled.

When virus definitions files are older than required or when Auto-Protect and heuristic virus scanning are disabled, client compliancy remediates the VPN client automatically. When the version of Symantec AntiVirus is too old, the issue is logged. In low risk environments, the client is allowed network access and the user is notified to upgrade. In high risk environments, the client is denied access and the user is notified to upgrade.

MIS also configures commands for the VPN's Administrative log to record all debug log events.

Chapter 3

Reset ACL tool

This chapter includes the following topics:

About the Reset ACL tool

Reset ACL (Resetacl.exe) lets you limit access to the Symantec AntiVirus registry key on Windows XP/2000/NT 4.0 computers.

By default, these computers allow all users to modify the data stored in the registry for any application, including Symantec AntiVirus. Reset ACL removes the permissions that allow full access by all users to the following Symantec AntiVirus registry key and its subkeys:

HKLM\SOFTWARE\Intel\LANDesk\VirusProtect6\CurrentVersion

Restricting registry access with the Reset ACL tool

You can use the Reset ACL tool to restrict registry access.

To restrict registry access with the Reset ACL tool

1. Roll out Resetacl.exe, located on the Symantec AntiVirus CD in the Tools folder, to unsecured computers.
2. Run Resetacl.exe on each of these computers.

After you have run Resetacl.exe, only users with Administrator rights can change the registry key values.

While the Reset ACL tool boosts security for Symantec AntiVirus on these computers, administrators should be aware that there are several trade-off considerations.

In addition to losing access to the registry, users without Administrator rights will not be able to do the following:

- Start or stop the Symantec AntiVirus service.
- Run LiveUpdate.
- Schedule LiveUpdate.
- Configure Symantec AntiVirus.
  For example, users cannot set Auto-Protect or email scanning options.

The options associated with these operations appear dimmed in the Symantec AntiVirus interface.

In addition, the user can modify scan options, but the changes are not saved in the registry or processed. The user can also save manual scan options as the default set, but the options are not written to the registry.

Chapter 4

Importer tool

This chapter includes the following topics:

About the Importer tool

The Importer tool (Importer.exe) identifies computers in a non-WINS environment to the Symantec System Center console. This lets Symantec AntiVirus locate computers during the network discovery process, when the names cannot be browsed using WINS/DNS. It is a command-line utility.

In addition to importing the paired names and IP addresses of computers located in non-WINS environments, you can add any other computer name and IP address pairing to the text file so that the computer is discovered in the future. For example, you may want to add the name and address of a computer that has not been discovered successfully for an unknown reason.

Note: In most cases, you should not need the Importer tool. The Find Computer feature of the Symantec System Center can usually find and identify Symantec AntiVirus servers on the network by means of address caching and the normal Discovery process.

How the Importer tool works

The Importer tool runs on any computer on which the Symantec System Center is installed. You can use it to import pairs of computer names and IP addresses from a text file into the address cache registry entries used by the Symantec System Center.

Once the computer name and address pairs are imported, entries are created in the registry under the following key:

HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDesk\VirusProtect6\CurrentVersion\AddressCache

You must run a Local Discovery or Intense Discovery after importing the data file. The Discovery queries the addresses of the computers. The computers running the Symantec AntiVirus server are added to the Discovery Service in memory and have complete entries created in the registry. The Discovery Service can then find the computers each time that the Discovery Service is run.

Where the Importer tool is located

The Importer tool consists of a single file, Importer.exe. Importer.exe is located on the Symantec AntiVirus CD in the Tools folder.

You can copy Importer.exe to any folder on a computer on which the Symantec System Center is installed, and then run it.

Importing addresses using the Importer tool

To import addresses to the address cache, you must be logged on with Administrator rights. This is necessary so that you have write access to HKEY_LOCAL_MACHINE.

Import addresses using the Importer tool

To import addresses using the Importer tool, you must complete the following tasks:

- Create a data file containing paired computer names and IP addresses.
- Run the Importer tool.

  Note: You must run the Importer tool from a command prompt.

- Run the Discovery Service.

To create a data file

1 Create a new file with a text editor such as Notepad.

2 Type the data in the following format:
<server name><comma><IP address><linefeed>
Avoid typing incorrect IP addresses for servers. No validation is performed to determine if two servers have the same IP address in the Importer text file.

3 Save the file.
For example, a data file named Computers.txt might look as follows:
Computer 1, 192.168.3.121
Computer 2, 192.168.3.122
Computer 3, 192.168.3.123
Computer 4, 192.168.3.124
Computer 5, 192.168.3.125
Computer 6, 192.168.3.126

Note: You can type a semicolon or colon to the left of an address to comment it out. For example, if you know that a network segment is down, you can comment out associated subnet addresses.

To run the Importer tool

1 At the command-line prompt, type the following command:
`<fullpath> importer <filename>`
where <fullpath> represents the full path to the Importer and <filename> represents the full path of the import file, such as C:\Computers\Computers.txt

2 Press **Enter**.

Deleting entries from the address cache

Data imported from the data file does not overwrite information that is already stored in the address cache. If you have data that should be overwritten, such as an incorrect computer address, clear the cache before running the Importer.

Note: After importing the contents of the data file, do not click Clear Cache Now. Doing so deletes the contents of the address cache, including the imported data.

To delete entries from the address cache

1. In the Symantec System Center console, on the Tools menu, click **Discovery Service**.
2. Under Cache Information, click **Clear Cache Now**.

Once you run Discovery after the data import, the correct data is available for future discovery sessions.

Advanced usage

The command line takes four parameters:

- Import file path
- First delimiter
- Second delimiter
- Order (1 = computer name/IP address, 2 = IP address/computer name; the default is 1)

Note: The second delimiter needs to be a single character only. For example, the ampersand cannot be used because the user would have to enter the following: “&”

For example, an import file named Machines.txt, in C:\MACHINES, could read as follows:

192.168.3.121/Server 1

192.168.3.122/Server 2

192.168.3.123/Server 3

The above example is in IP address/computer name order (2). The first parameter is a slash (/) and the second is a linefeed. The corresponding syntax for the command line would be:

importer C:\MACHINES\Machines.txt / LF 2

After the computer name and IP address pairs are imported, entries are created in the registry under the following key:

HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDesk\VirusProtect6\CurrentVersion\AddressCache

You must run a local or intense discovery after importing the data file. The discovery queries the computer IP addresses. The computers running Symantec AntiVirus are added to the Discovery Service in memory and have complete

entries created in the registry. The Discovery Service can then find the computers each time that the Discovery Service is run.

Getting Help while using the Importer tool

You can access Help on Importer switch and syntax information.

To get Help while using the Importer tool

1. At the command line, type the following:
   `Importer`
2. Press **Enter**.

The Importer tool displays the following Help information:

```
Simple Usage : IMPORTER <filename>
<filename> : full path of import file
File format : <server name><comma><ip address><linefeed>
Example File : Server 1,192.168.3.121
Server 2,192.168.3.122
Server 3,192.168.3.123
press "a" for advanced usage
When "a" is pressed for advanced usage, the following help will be
displayed:
Advanced Usage: IMPORTER <filename> <delimiter 1> <delimiter 2>
<order>
<filename> : full path of import file
<delimiter 1> : separator between first and second item in pair
<delimiter 2> : separator between pairs
NOTE: for carriage return/linefeed delimiters, use LF
for space delimiters, use SP
for comma, use ,
<order> : order of computer name/ip address pairs
1 = computer name/ip address order
2 = ip address/computer name order
EXAMPLE -
File contents : 192.168.3.121/Server 1
192.168.3.122/Server 2
192.168.3.123/Server 3
Command line : IMPORTER C:\MyFolder\MyFile.txt / LF 2
```

Known problems

Importer depends on the HKLM\SOFTWARE\Intel\LANDesk\VirusProtect6\CurrentVersion\AddressCache key used by the Symantec System Center. If this key is not present, an error message appears.

The Importer modifies the AddressCache key under HKLM, so the user needs local administrator rights.

The Importer tool aids in the discovery process of the Symantec System Center. The Importer determines whether the Symantec System Center is present on the local computer. If not, an error message appears.

After an import, the computer names paired with their IP addresses in the registry are not complete. They show only the computer under the Address_0 and Protocol dword values. A discovery must be run to complete the process (using the Run Discovery Now button in the Discovery Service Properties dialog box).

Do not click the Clear Cache Now option in the Discovery Service Properties dialog box. This deletes the contents of the address cache, including the imported data.

The Importer cannot assist in locating computers during the installation process.

Note: When you are pushing the Symantec AntiVirus client and server to remote computers, an Import option appears in the Select Computer dialog box. Do not confuse this Import option with the Import option on the NT Client Install and AV Server Rollout installation screens.

The Importer does not overwrite existing IP addresses in the address cache; this is an intended design feature. However, there is a possibility that an incorrect IP address may exist in the cache. In such a case, the Importer cannot correct it.

Chapter 5

Windows XP/2000/NT services

This chapter includes the following topics:

Symantec AntiVirus services

Table 5-1 lists the names and descriptions for Symantec AntiVirus server services. These appear in the Windows XP/2000/NT Services control panel.

Table 5-1 Symantec AntiVirus server services

Service name	Binary name	Description
Symantec AntiVirus Server	Rtvscan.exe	Main Symantec AntiVirus service. Most Symantec AntiVirus server-related tasks are performed in this service.
Defwatch	Defwatch.exe	Service that watches for newly arriving virus definitions. Launches a scan of the files in Quarantine when the new virus definitions arrive.
Intel PDS	Pds.exe	Ping Discovery Service. Allows Discovery of Symantec AntiVirus on this computer to occur. Applications register with this service, along with an APP ID, and a pong packet to return in response to ping requests.

Table 5-2 lists the names and descriptions for Symantec AntiVirus client services. These appear in the Windows XP/2000/NT Services control panel.

Table 5-2 Symantec AntiVirus client services

Service name	Binary name	Description
Symantec AntiVirus Client	Rtvscan.exe	Main Symantec AntiVirus service. Most Symantec AntiVirus client-related tasks are performed in this service.
Defwatch	Defwatch.exe	Service that watches for newly arriving virus definitions. Launches a scan of the files in Quarantine when the new virus definitions arrive.
Client roaming service	Savroam.exe	Provides roaming server data to roaming clients.
Common client event manager	CcEvtMgr.exe	Client event manager POP3 scanning.
Common client password service	CcPwdSvc.exe	Client password service POP3 scanning.
Common client settings manager	CcSetMgr.exe	Encrypted client settings storage for POP3 scanning.
Common client Symantec Network Drivers	SNDSrvc.exe	Symantec Network Drivers for POP3 scanning.
Configuration Wizard service	CfgWzSvc.exe	This service appears in the Windows Task Manager Processes when an installation fails. The service normally deletes itself after the Symantec AntiVirus Configuration Wizard runs.

Symantec System Center services

Table 5-3 lists the names and descriptions for Symantec System Center services. These appear in the Windows XP/2000/NT Services control panel.

Table 5-3 Symantec System Center services

Service name	Binary name	Description
Symantec System Center Discovery Service	Nsctop.exe	Discovery Service used to find Symantec AntiVirus servers on the network. The Discovery Service also populates the console with objects.

Table 5-4 lists the names and descriptions for Alert Management System^2 services. These appear in the Windows XP/2000/NT Services control panel.

Table 5-4 Alert Management System^2 services

Service name	Binary name	Description
Intel Alert Handler	Hndlrsvc.exe	AMS^2 Alert Handler service. Provides alerting actions such as message boxes, pages, emails, and so on.
Intel Alert Originator	Iao.exe	AMS^2 Alert Originator service. Lets alerts be received on this computer. Alerts can be received from either the local computer (in the case of a primary server), or from a remote computer (in the case of unmanaged clients using a centralized AMS^2 server).
Intel File Transfer	Xfr.exe	File transfer service. Provides file transfer capabilities to AMS^2.
Intel PDS	Pds.exe	Ping Discovery Service. Allows Discovery of Symantec AntiVirus on this computer to occur. Applications register with this service, along with an APP ID, and a pong packet to return in response to ping requests.

Chapter 6

Windows XP/2000/NT Event Log entries

This chapter includes the following topics:

Symantec AntiVirus events

Table 6-1 lists events written by Symantec AntiVirus to the Windows XP/2000/NT Event Log.

Table 6-1 Events written to the Windows Event Log

Event	Event number	Description
Scan Stopped	2	Occurs when scanning completes.
Scan Started	3	Occurs when scanning starts.
Definition File Sent To Server	4	Occurs when a parent server sends a .vdb file to a secondary server.
Virus Found	5	Occurs when scanning detects a virus.
Scan Omission	6	Occurs when scanning fails to gain access to a file or directory.
Definition File Loaded	7	Occurs when Symantec AntiVirus loads a new .vdb file.

Table 6-1 Events written to the Windows Event Log

Event	Event number	Description
Virus Behavior Detected	11	Occurs when Auto-Protect email scanning handles email attachments.
Configuration Changed	12	Occurs when a server updates its configurations according to the changes made from the console, excluding configuration changes made in the PRODUCTCONTROL or DOMAINDATA registry keys.
Symantec AntiVirus Shutdown	13	Occurs when the Symantec AntiVirus service is unloaded.
Symantec AntiVirus Startup	14	Occurs when the Symantec AntiVirus service is loaded.
Definition File Download	16	Occurs when new definitions are downloaded by a scheduled definitions update.
Scan Action Auto-Changed	17	Occurs when Symantec AntiVirus has deleted or quarantined more than 5 infected files within the last minute. The number of files quarantined or deleted and the time interval are configurable from the registry. The defaults are 5 files in 60 seconds.
Sent To Quarantine Server	18	Occurs when quarantined files are sent to a Quarantine Server.
Delivered To Symantec Security Response	19	Occurs when a file is delivered to Symantec Security Response.
Backup Restore Error	20	Occurs when Symantec AntiVirus cannot back up a file or restore a file from Quarantine.
Scan Aborted	21	Occurs when a scan is stopped before it completes.
Symantec AntiVirus Auto-Protect Load Error	22	Occurs when Auto-Protect fails to load.

Table 6-1 Events written to the Windows Event Log

Event	Event number	Description
Symantec AntiVirus Auto-Protect Loaded	23	Occurs when Auto-Protect loads successfully.
Symantec AntiVirus Auto-Protect Unloaded	24	Occurs when Auto-Protect is unloaded.
Removed Client	25	Occurs when a parent server removes a client computer from its clients list. This will happen by default when a client computer fails to check in with its parent server for over thirty days.
Scan Delayed	26	Occurs when a scheduled scan is snoozed (delayed).
Scan Re-started	27	Occurs when a snoozed/paused scan is restarted.
Roaming Client added to Server	28	Occurs when a roaming client is added to a server.
Roaming Client deleted from Server	29	Occurs when a roaming client is removed from a server.
License Warning	30	Occurs when a license warning message is generated.
License Error	31	Occurs when there is a license error.
Access Denied Warning	33	Occurs when an unauthorized communication attempt is made.
Log Forwarding Error	34	Occurs when there is a problem with the log forwarding process.
License Installed	35	Occurs when a license is installed.
License Allocated	36	Occurs when a license is allocated.
License Status	37	Occurs when a license is validated.

Index